Symantec Endpoint Encryption Full Disk Release Notes

Symantec Endpoint Encryption Full Disk 8.0.1.SP1
Symantec Endpoint Encryption Framework 8.0.1.SP1
www.symantec.com

About Symantec Endpoint Encryption Full Disk

Symantec Endpoint Encryption Full Disk protects data on laptops and PCs from the threat of theft or loss with strong, centrally managed encryption, auditing, and policy controls for full disks and partitions, ensuring that the loss of a machine and its data does not result in disclosure required by corporate policy or government regulation.

Symantec Endpoint Encryption Full Disk provides the industry's most robust and comprehensive integration with Microsoft Active Directory for fast, simple deployment of endpoint data protection controls in a familiar administrative environment.

Installation Notes

Symantec Endpoint Encryption Framework 8.0.1.SP1 is only compatible with Symantec Endpoint Encryption Full Disk 8.0.1.SP1 and Symantec Endpoint Encryption Removable Storage 8.0.1.SP1. If you are running Symantec Endpoint Encryption Removable Storage and plan to upgrade to Symantec Endpoint Encryption Full Disk 8.0.1.SP1, you must also upgrade to Symantec Endpoint Encryption Removable Storage 8.0.1.SP1.

Resolved Issues

Number	Description
	USB/Boot incompatibilities have been resolved for the following:
MA22227	Lenovo W510 4389W3J
MA22911	Lenovo T410
MA23094	GETAC B300
MA23163	Dell Precision M4500
MA23208	Lenovo M90p
MA23333	Lenovo Y410
MA23347	Dell Inspiron 580S
MA23348	Panasonic CF-F9KWHZG2M
MA23382	Fujitsu P770
MA23393	Lenovo W701
MA23402	HP mini - 210-1075ca
MA23414	HP Elite Book 8440W
MA23430	Panasonic CF-T8EWDTZAM
MA23431	Lenovo T410-2522-25U
MA23433	Lenovo X201-3626-11U
MA23434	Dell Optiplex 980
MA23437	Sony Vaio VGN-SZ740
MA23440	HP Z400 does not boot into Safe Mode
MA23448	Dell Precision T1500
MA23449	Panasonic CF-F8
MA23254	HP 8540W
MA23449	Panasonic CF-F8GWE08N3
MA23456	Toshiba NB305
MA23485	Dell 5400 and 5410
MA23537	Dell E5500
MA23599	Lenovo Thinkpad T410
MA23602	Lenovo T510 431328U
MA23603	Lenovo M58
MA23604	Lenovo M70
MA23605	Lenovo X201 3680AU9
MA23641	HP touch Smart USB keyboard mouse

Known Issues

Third Party Compatibility—Hardware

Number	Hardware	Description	Workaround
MA21992	HP Mini 2102	The HP Mini 2102 may fail to boot up following disk encryption.	Do not encrypt the HP Mini 2102.
MA21929	Dell XPS 1320	If Windows 7 is installed, the computer will fail to boot into Windows following the installation of Symantec Endpoint Encryption Full Disk.	Do not deploy Symantec Endpoint Encryption Full Disk to the Dell XPS 1320 if Windows 7 is installed.
MA23309	Dell E6510 with Windows 7 64-bit Editions	Dell E6510 machines running 64-bit Editions of Windows 7 may be unable to resume after hibernation.	Power off.

Number	Hardware	Description	Workaround
MA21884 MA21864	HP Compaq dc5700 and dc5100	If multiple USB devices are inserted at boot time, the computer will fail to boot into Windows.	Remove USB devices and try again.
MA21327	Panasonic Toughbook CF-U1AQB1GAM	Users will be unable to use USB devices such as keyboards and mice during pre-Windows authentication.	Users should open laptop and use the internal keyboard and mouse pad to complete pre-Windows authentication.
MA22221	HP EliteBook 8740w	Users will be unable to use USB 3.0 devices such as keyboards and mice during pre-Windows authentication.	
MA21514	Dell Latitude D631 and D531	Following the removal of the CD/DVD drive, the computer will fail to boot into Windows.	Uninstall Symantec Endpoint Encryption Full Disk before removing the CD/DVD drive.
MA20752	SanDisk 4GB Cruzer Micro USB Flash Drive and HP Compaq dc7700	A SanDisk 4GB Cruzer Micro USB Flash Drive inserted at startup will cause HP Compaq dc7700 computers to hang after Pre-Windows authentication.	Remove SanDisk devices before powering on.
MA19704	SanDisk Cruzer Micro 512 MB USB 2.0 Flash Drive (SDCZ4-512-A10)	If the SanDisk Cruzer Micro 512 MB USB 2.0 Flash Drive (SDCZ4-512-A10) device is inserted at startup, users may experience slow boot times.	Remove SanDisk devices before powering on.

Third Party Compatibility—Software

Number	Third Party Tool	Description	Workaround
—	Roxio 6.2	The Framework client package will fail to install due to a missing drive letter in the primary partition.	Ensure that the following Registry key has the value **PartMgr**: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4D36E967-E325-11CE-BFC1-08002BE10318}\UpperFilters
MA15919	Symantec Endpoint Protection 11	Following the installation of Symantec Endpoint Encryption Full Disk on the Client Computer, a **Network Threat Protection** message may be displayed, alerting the end user to a change in the EAFRCliADSI application.	Open Symantec Endpoint Protection and click **Options** in the **Network Threat Protection** area. Select **Configure Firewall Rules** from the pop-up menu. Highlight **Block IPv6 over IPv4** and click **Edit**. Select the **Allow this traffic** option button on the **General** tab. Open the **Ports and Protocols** tab. Select **All IP Protocols** from the **Protocol** drop-down list box.
MA12457	RSA SecurID® 800	If a second certificate is added to the token and the first certificate is deleted, the user will be unable to register with the token.	Remove all certificates from the token and add the certificate again.

Upgrade/Install/Uninstall/Migration

Number	Description	Workaround
MA23202	Novell users with Single Sign-On enabled may have to manually log on to Novell following an upgrade to this version of Full Disk.	Instruct the user to open the Novell SSO panel and select the **Reset Single Sign-On to Novell Netware** check box.
MA22161	If a custom destination folder was chosen during the installation of GuardianEdge Management Server 9.2.2, 9.2.1, or 9.2.0, the default path shown in the **Destination Folder** page during the upgrade to 7.0.7 will be missing the final subdirectory. For example, if you chose C:\GuardianEdge\Management Server\ for your original installation files, C:\GuardianEdge will be the default.	Click **Change** and navigate to the desired destination of the Symantec Endpoint Encryption Management Server files.
MA20747	If a local instance is selected during the installation of the Symantec Endpoint Encryption Management Server, Symantec Endpoint Encryption Management Server uninstallation will fail with the message, "Could not connect to Microsoft SQL Server."	Locate the GEServerConfig.xml file on the Symantec Endpoint Encryption Management Server machine. Find **(local)**. Replace with the computer name of the Symantec Endpoint Encryption Management Server machine. Save and close the file. Try the uninstall again.
MA15465	If power is lost during an upgrade or migration of the client machine, a blue screen may occur and the machine may loop continuously in an effort to boot into Windows.	Run Recover /d. If Recover /d fails, try Recover /b. If the Recover Program completes successfully, back up important files, then uninstall Encryption Plus Hard Disk or reinstall Symantec Endpoint Encryption Full Disk. If this fails, you will need to reinstall Windows or reimage the machine.
MA12748	If password authentication is selected during the installation of Symantec Endpoint Encryption Framework Manager console, but token authentication is specified by policy, users will be unable to register.	
MA16499	Following the successful application of a Symantec Endpoint Encryption migration package to an Encryption Plus Hard Disk 7.0.23, 7.1.0, or 7.1.1 workstation, users will need to log on to Encryption Plus Hard Disk one last time.	

Token Authentication

Number	Description	Workaround
MA19987 MA20673	Tokens cannot be used for Pre-Windows authentication on the Acer Aspire 5515.	
MA21516	The GemPC Express reader cannot be used for Pre-Windows authentication on an HP Compaq 6535b.	

Drive Fragmentation

Number	Description	Workaround
MA21057	The following error message is displayed on the first reboot after installation, "EPHD BIOS Translation Driver: heap allocation error."	One or more drives are severely fragmented. Decrypt all drives. Uninstall Symantec Endpoint Encryption Full Disk. Defragment the drive(s). Reinstall Symantec Endpoint Encryption Full Disk.

Mac Endpoints

Number	Description	Workaround
BU29702	Any user on a Mac client can change the password of any another user on the same Mac client.	
MA23248	The Symantec Endpoint Encryption Full Disk client application will stop functioning following receipt of a policy containing a Client Administrator whose name is the same as one of the users.	Create and apply a new policy containing a Client Administrator with a name different than any existing or potential user.
MA23418	The latest Mac operating system version number won't be displayed in the Manager Console if the operating system is upgraded after a policy has already been assigned.	Move the Mac computer to the Unassigned group and back again to refresh the value.
BU25451 BU25612	Users who restart to complete a software update during disk encryption may experience difficulty booting.	Turn off automatic updates during disk encryption. If difficulty booting occurs, use target disk mode.
BU28838	A **Certificate Trust** prompt displays following the installation of Symantec Endpoint Encryption Full Disk on the Mac, if HTTPS communications are configured.	Provide administrative credentials and accept the changes.
BU24999	Kernel panic occurs if an encrypted disk is erased or reformatted.	Decrypt the disk before erasing or reformatting it.
BU11936	NitroAV PCMCIA/FireWire 800 removable devices will be unavailable for encryption.	
BU28805	Disks may disappear from the list of drives after being encrypted and decrypted many times.	Close PGP Desktop and then reopen PGP Desktop.
BU28780	The PGP Desktop icon will not be displayed for additional users.	Additional users must open PGP from the Applications folder once for the PGP Desktop icon to be displayed.
BU28815	Decryption does not begin when the user clicks **Decrypt** while re-encrypting, the re-encryption process merely pauses.	Click **Resume** to resume re-encryption and decrypt after re-encryption completes.
BU28925 BU28943	All users may not always be displayed in the **User Access List** in PGP Desktop, such as after a successful WDRT process or when a number of users are added.	Press OPTION as you select the PGP icon in the menu bar and select **Quit**. Then locate the PGP Desktop application on your system (usually in the Applications folder) and double-click the file.

Number	Description	Workaround
BU28944	After reinstalling Symantec Endpoint Encryption Full Disk or gaining access to the Mac OS X system using the Whole Disk Recovery Token (WDRT), a message indicating that the PGP Engine has stopped may be displayed and/or the PGP Desktop icon may disappear from the menu bar.	Locate the PGP Desktop application on your system (usually in the Applications folder) and double-click the file.

Windows Power Management

Number	Description	Workaround
MA21816	Autologon may not succeed on Windows 7 endpoints following hibernation of the endpoint—if the **Disengage if power lost for ▢ minutes** check box is selected.	To achieve successful Autologon on Windows 7 endpoints, ensure that only complete shut downs or restarts are performed for the duration of the Autologon GPO policy—if the **Disengage if power lost for ▢ minutes** check box is selected.
MA18851	Following the installation of Symantec Endpoint Encryption Full Disk, Vista computers missing the **Sleep** power option will go into hibernation on a schedule that does not correspond to the Windows power plan.	Apply all of the latest Vista updates.

Safe Mode Reboot Option

Number	Description	Workaround
MA21491	The Safe Mode reboot option may fail to allow administrators to access safe mode on certain machines, such as the HP Compaq dc5800.	Reboot. Provide Client Administrator credentials and select the **Safe Mode Reboot** check box. Click **OK**. Click **Restart Computer**. Watch screen closely. As soon as "Starting SEE Full Disk…" displays, press F8. Select **Safe Mode**. Press F8. Select **Safe Mode** again.

Manager Console

Number	Description	Workaround
MA23154	Removable devices encrypted using Full Disk on a Mac client will be listed in the **Fixed Drives** tab as many times as they are encrypted.	
MA21307	If an XPS print job is cancelled, the following error may be displayed, "The data area passed to a system call is too small."	
MA20559	After clicking a column heading to sort by the column, the sort arrow will be displayed to the left of the column heading if the operating system is Vista or Server 2008.	

Number	Description	Workaround
MA16623	Deploying an Active Directory policy that contains a change to the Client Administrator settings from a Symantec Endpoint Encryption 6.1.0 or later Manager to Symantec Endpoint Encryption 6.0.0 or earlier and/or GuardianEdge Framework 8.5.3 or earlier clients will result in a failure of the new Client Administrator policy to be applied, a deletion of all existing Client Administrator policies, and a return to the Client Administrators specified in the original installation settings.	When deploying an Active Directory policy from a 6.0.0 or earlier Manager, add the following WMI filter: **Select * FROM Win32_Product WHERE (name="Symantec Endpoint Encryption Framework Client" AND Version <= "6.0.0") OR (name="GuardianEdge Framework Client" OR name="Encryption Anywhere Framework Client") AND version <= "8.5.3"))** When deploying an Active Directory policy from a 6.1.0 or later Manager, add the following WMI filter: **Select * FROM Win32_Product WHERE (name = "Symantec Endpoint Encryption Framework Client" AND version > "6.1.0") OR (name = "GuardianEdge Framework Client" AND version > "9.0.0")**

Client Keyboards

Number	Description	Workaround
MA19021	Users may be unable to combine the ^ (Circumflex), ¨ (Diaeresis), ` (Grave) and ´ (Acute) dead keys with l (0131), I (0049), Shift+i (0069) or Shift+I (0130) from the Turkish Q keyboard.	
MA19019	The Turkish Q character İ; (0130) may display as I in pre-Windows.	
MA16958	Users will be unable to enter the following characters from Canadian French keyboards in Pre-Windows: á ç	
MA18893	The CAPSLOCK key will behave like the SHIFTLOCK key for non-alphabet characters in Pre-Windows for the Belgian (Period), French, and German keyboards.	
MA19067	The character ł (0142) displays as Ł (0141) in pre-Windows when the Hungarian keyboard is used.	
MA19335	CTRL+ALT combinations do not produce the expected special characters in Pre-Windows.	
MA23142	If the Portuguese (Brazil) character ₢; (0x20A2) displays as a box with a hex character inside during Pre-Windows authentication.	Ignore the incorrect display.

Single Sign-On

Number	Description	Workaround
MA15304 MA15302	If a user presses CRTL+ALT+DEL in Windows Vista, clicks **Change Password**, provides the incorrect old password causing an error or is prevented from changing their password due to Windows policies, and then cancels out, that user will be unregistered from Symantec Endpoint Encryption.	Visit *http://support.microsoft.com/kb/936183*. Obtain and apply the hotfix.

Pre-Windows Help and Keyboard Layout Windows

Number	Description	Workaround
MA18231	Users will not be able to utilize the Keyboard Layout window if Help is open.	Close the Help window and try again.

Section 508

Number	Description	Workaround
MA16937	JAWS does not always announce all of the information displayed within the Registration wizard and User Client consoles.	Users should follow these steps: 1. Press INSERT+F9. 2. Select the frame that is of interest from the resultant **Frames List** dialog. 3. Click **OK**. 4. Press P. If this doesn't work, restart JAWS and try the steps again.

Legal Notice

Copyright © 2011 Symantec Corporation. All rights reserved. Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. GuardianEdge and Encryption Anywhere are either registered trademarks or trademarks of GuardianEdge Technologies Inc. (now part of Symantec) in the U.S. and/or other countries. Other names may be trademarks of their respective owners.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation," as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

Symantec Corporation
350 Ellis Street

Mountain View, CA 94043
http://www.symantec.com